CLAIMS

What is claimed is:

1. A method comprising:

receiving input data;

determining if a salt value exists;

generating a salt value and storing the salt value in a table entry if the salt value does not exist;

retrieving the salt value from the table entry if the salt value exists;

generating a hash from the salt value and the input data;

generating a password from the hash; and

returning the password to an application to gain entry to the application.

2. The method of claim 1, wherein the input data comprises a user identification and a strong password.

3. The method of claim 2, wherein the input data further comprises an application identification.

4. The method of claim 2, further comprising determining if a new strong password is required; and

retrieving the new strong password if the new strong password is required.

5. The method of claim 2, wherein the strong password is used to generate a plurality of application passwords.

6. The method of claim 1, wherein the salt value is one of predetermined and generated by a random number generator.

7. The method of claim 1, wherein the salt value and the application are associated in the table entry.

8. The method of claim 1, wherein the application is run on one of a local computer system and a networked computer system.

9. The method of claim 1, wherein one of a secure hash algorithm (SHA-1) and a message digest (MD5) algorithm are used to generate the hash.

10. The method of claim 1, wherein the generated password is temporarily stored in a memory for a predetermined time period.

11. The method of claim 10, wherein the predetermined time period is based on platform activity.

12. The method of claim 11, wherein the platform is one of a local computer system and a networked computer system.

13. A program storage device readable by a machine comprising instructions that cause the machine to:

receive input data;

determine if a salt value exists;

generate a salt value and store the salt value in a table entry if the salt value does not exist;

retrieve the salt value from the table entry if the salt value exists;

generate a hash from the salt value and the input data;

generate a password from the hash; and

return the password to an application to gain entry to the application.

14. The program storage device of claim 13, wherein the input data comprises a user identification and a strong password.

15. The program storage device of claim 14,wherein the input data further comprises an application identification.

16. The program storage device of claim 13, further comprises instructions that cause the machine to:

determine if a new strong password is required; and

retrieve the new strong password if the new strong password is required.

17. The program storage device of claim 16, wherein the strong password is used by the machine to generate a plurality of application passwords.

18. The program storage device of claim 13, wherein the salt value is one of predetermined and generated by a random number generator.

19. The program storage device of claim 13, wherein the salt value and the application are associated in the table entry.

20. The program storage device of claim 13, wherein one of a secure hash algorithm (SHA-1) and a message digest (MD5) algorithm are used in instructions to cause the machine to generate the hash.

21. The program storage device of claim 13, wherein the generated password is temporarily stored in a memory for a predetermined time period.

22. The program storage device of claim 21,wherein the predetermined time period is based on platform activity.

23. The program storage device of claim 22, wherein the platform is one of a local computer system and a networked computer system.

24. A method comprising:

receiving a user password;

receiving a name of an application requiring a password;

determining a correct salt value for the application;

computing an application dependent password for a user, wherein the application dependent password depends on the user password and the salt value for the application; and

returning the application dependent password to the application.

25. The method of claim 24, wherein the computing of the application dependent password depends on a user name.

26. The method of claim 25, wherein the computation of the application dependent password further includes hashing the user name, the user password, and the salt value for the application.

27. The method of claim 25, further comprising retrieving an old password if the old password is required.

28. The method of claim 25, wherein a strong password is used to generate a plurality of application passwords.

29. The method of claim 24, wherein the salt value is unique for a user and an application.